Functional Series 500 - Management Services
Chapter 545 - Information Systems Security

Table of Contents

* Asterisks indicate that the adjacent material is new or substantively revised.

Chapter 545 - Information Systems Security

545.1 OVERVIEW

Effective Date: 06/27/2001

This chapter outlines the basic policies that underlie the Agency's Information Systems Security (ISS) Program. This chapter documents the Agency's primary ISS policy for systems used to process unclassified data. Some forms, formats, and guidance in ADS 545 also apply to classified USAID information systems (IS). Other guidance for classified data processing is contained in ADS 552, Classified Information Systems Security.

This chapter contains the following:

- USAID's overall policies and procedures to protect unclassified IS;
- General IS access procedures (personnel, technical, and administrative security requirements for unclassified USAID networks);
- Selected procedures for access to and processing Sensitive But Unclassified (SBU) data, and computer operations overseas and in special threat areas (to include guidance on contingency response requirements); and
- Details on USAID facsimile and networking security requirements.

545.2 PRIMARY RESPONSIBILITIES

Effective Date: 04/25/2002

Law and Federal guidance require agencies to incorporate security into their information technology architectures and the life cycles of their information systems. More detailed security responsibilities apply to Mission Critical Systems and National Security Systems (see 545.6, Definitions, for statutory and regulatory terms that apply to information systems). Within USAID, primary information systems security (ISS) responsibilities are as follows:

a. The Administrator is responsible for developing and implementing a comprehensive, Agency-wide ISS program that is technically current, cost effective, and in full compliance with established national security directives. This responsibility has been delegated to the Director, Bureau for Management, Office of Information Resources Management (M/IRM). The Administrator is also responsible for designating the Information Systems Security Officer (ISSO) for USAID. More details on Agency ISS responsibilities are contained in the Internal Mandatory Reference, "Information Technology Security Roles and Responsibilities." (See Mandatory Reference, **Information Technology Security Roles and Responsibilities**)

b. The Assistant Administrator, Bureau for Management (AA/M) serves as the Chief Information Officer (CIO). The CIO is responsible for directing, managing, and providing

policy guidance and oversight with respect to all Agency information resource management activities. These responsibilities may be delegated to senior-level office managers. The CIO serves as the system Certification and Accreditation (C&A) process Designated Security Accreditation Authority (DSAA) for most of USAID's IS, including IS at USAID Missions, and will oversee both annual IT program reviews and any Agency-wide reports to OMB on IT security issues.

NOTE: Details on the Certification and Accreditation process are included in the Internal Mandatory Reference, "Information Systems Certification and Accreditation, Approval to Operate." (See Mandatory Reference, **Information Systems Certification and Accreditation, Approval to Operate**)

c. The Director, Office of Financial Management (M/FM), USAID's Chief Financial Officer (CFO), serves as the DSAA for financial IS in USAID/Washington (USAID/W).

d. The Director, Bureau for Management, Office of Information Resources Management (M/IRM) is responsible for providing "signatory approval to operate" for all information systems used to process, store, or print Sensitive But Unclassified information. The Director of M/IRM has the authority to approve, subsequent to coordination with the Director of the Office of Security (D/SEC), the use of all information systems used to process, store, or print classified national security information. Other USAID IS-related functions assigned to the Director of M/IRM are contained in the Mandatory Reference, **Information Technology Security Roles and Responsibilities.**

e. The ISSO for USAID is designated by the Administrator and is directly responsible for overseeing and executing the bulk of the Agency's operational information systems security activities. In addition, USAID's ISSO, after consultation with the Office of Security (SEC), is responsible for developing and implementing methodologies for

- Detecting, reporting, and responding to IS security incidents;
- Notifying the Office of Inspector General about IS security incidents involving any apparent violation of laws, rules, or regulations; and
- Notifying and consulting with other offices and authorities, to include the General Services Administration's Federal Computer Incident Response Capability (FedCIRC), in the event that a significant IS security incident occurs.

f. Program Managers and Mission Directors have management responsibilities for USAID IS used to execute their Mission's and program's operations. They must appoint U.S. citizens with SECRET security clearances as designated ISSOs and alternate ISSOs to implement the Agency's information systems security policies and guidelines for their programs and Missions. The designated ISSO at USAID Missions is usually

the Executive Officer (EXO); however, a Mission Director may appoint another U.S. citizen with a SECRET clearance as designated ISSO instead.

g. The Director, Office of Security (D/SEC) is responsible for providing technical guidance and security policy determinations on issues within SEC's assigned responsibilities.

h. The Office of Inspector General (OIG), consistent with legal and regulatory guidance, conducts evaluations of USAID IS.

i. Other USAID organizations and individuals have responsibilities for IS security functions, such as --

- The Bureau for Management, Office of Information Resources Management, Telecommunications and Computer Operations Division (M/IRM/TCO);
- The Bureau for Management, Office of Information Resources Management, Systems Development and Maintenance Division (M/IRM/SDM);
- Certification Authorities, which include Mission Directors at USAID Missions, certify IS that support operations conducted in their organizations;
- Designated ISSOs within USAID organizations, Information Technology (IT) Specialists (USAID/W), System Managers (USAID Missions), IT system staff, and users.

545.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

Effective Date: 06/28/2002

The Office of Management and Budget (OMB) revised its Circular A-130, Appendix III effective November 28, 2000. (See Mandatory Reference, **OMB A-130, Appendix III**) In accordance with OMB guidance, agencies must

- Prioritize key systems (including those that are most critical to agency operations); and
- Apply OMB policies for non-national security applications and National Institute of Standards and Technology (NIST) guidance to achieve adequate security commensurate with the level of risk and magnitude of harm.

Agencies must make security's role explicit in information technology investments and capital programming. Investments in the development of new, or the continued operation of existing, information systems, both general support systems and major applications, must

- Demonstrate that the security controls for components, applications, and

systems are consistent with, and an integral part of, the Enterprise Architecture (EA) of the agency;

- Demonstrate that the costs of security controls are understood and are explicitly incorporated into the life-cycle planning of the overall system in a manner consistent with OMB guidance for capital programming;

- Incorporate a Mission, site, or system security plan that complies with Appendix III of OMB Circular A-130, is consistent with NIST guidance, and includes the development of rules, security training, and the implementation of operational, management, and technical controls (see the Mandatory Reference, **Information Technology Security Roles and Responsibilities,** for more information);

- Demonstrate specific methods used to ensure that risks and the potential for loss are understood and continually assessed, that steps are taken to maintain risk at an acceptable level, and that procedures are in place to ensure that controls are implemented effectively and remain effective over time;

- Demonstrate specific methods used to ensure that the security controls are commensurate with the risk and magnitude of harm that may result from the loss, misuse, or unauthorized access to or modification of the system itself or the information it manages;

- Identify additional security controls that are necessary to minimize risk to and potential loss from those systems that promote or permit public access, other externally accessible systems, and those systems that are interconnected with systems over which program officials have little or no control;

- Deploy effective security controls and authentication tools consistent with the protection of privacy, such as public-key-based digital signatures, for those systems that promote or permit public access;

- Detect, report, and respond to information system security incidents in accordance with section **545.3.6.8** and the guidance provided in the Mandatory Reference, **Incident Response Guidance for Unclassified Information Systems;**

- Ensure that the handling of personal information is consistent with relevant government-wide and agency policies; and

- Describe each occasion when the agency decides to employ standards and guidance that are more stringent than those promulgated by NIST to ensure the use of risk-based cost-effective security controls for non-national security applications.

OMB will consider for new or continued funding only those system investments that satisfy these criteria. New information technology investments must demonstrate that existing agency systems also meet these criteria in order to qualify for funding.

545.3.1 Information Systems (IS) Protection

Effective Date: 06/27/2001

It is the policy of the United States Agency for International Development (USAID) to protect the Agency's electronic information commensurate with the risk and magnitude of harm that would result from the loss, misuse, or unauthorized access to or modification of such information. All data of value to the Agency requires some minimum level of protection. Certain data, because of the sensitivity or criticality of the information to the mission of USAID, requires additional safeguards.

The Agency's policy is to implement and maintain an Information Systems Security (ISS) Program to ensure that adequate computer security is provided to all Agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. All USAID networked computer systems must provide controlled access protection safeguards to protect the integrity, availability, and, where required, the confidentiality of Agency information.

545.3.1.1 Information Systems Security (ISS) Program

Effective Date: 06/27/2001

USAID’s ISS Program implements policies, standards, and procedures that are consistent with government-wide policies, standards, and procedures issued by the Office of Management and Budget, the Department of Commerce, the General Services Administration, and the Office of Personnel Management. Different or more stringent requirements for securing national security information will be incorporated into USAID classified programs as required by appropriate national security directives. Classified processing requirements do not apply to unclassified systems. However, at a minimum, USAID’s ISS Program requires that the controls outlined in OMB A-130, and its Appendix III, must be implemented in all Agency general support and major applications systems. (See Mandatory Reference, **OMB Circular A-130, and its Appendix III**)

545.3.1.2 Access to Unclassified IS Networks

Effective Date: 06/27/2001

USAID's security policy for access to unclassified USAID computer networks is designed to protect sensitive Agency information against unauthorized access or disclosure. USAID implements this policy by using formal authorized access permission procedures based on a clearly demonstrated need-to-know or need-to-use determination for every person granted access to a USAID IS. USAID's security policy is supported by an approved personnel screening process and formal authorization approval. When all these factors are used together, they implement the USAID security policy for USAID System access.

545.3.1.3 Security Responsibilities for Unclassified IS Networks

Effective Date: 06/27/2001

For each general support system and major application system, USAID management is required to --

- Assign responsibility for security;
- Develop, document, and implement system security plans;
- Review security controls; and
- Authorize processing.

545.3.2 Unclassified Information Processing

Effective Date: 04/25/2002

All personnel with information systems security responsibilities must adhere to personnel, technical, administrative, and physical security policies and procedures when USAID equipment is used to support Agency objectives.

- Personnel security aspects of ISS require determinations as to an individual's personal reliability and trustworthiness, as well as identification of his or her need to know and access particular types of data in order to perform his or her assigned functions.
- Technical security aspects of ISS require implementation of technological methodologies in order to ensure data is accessible, is verifiable, and is secure from unauthorized access or damage.
- Administrative security aspects of ISS require documentation of critical security actions as they are completed to demonstrate compliance.
- Physical security aspects of ISS protect hardware, software, and other IS components from damage or loss (to include loss due to negligence or intentional misconduct).

Note: To assist individuals working outside the information technology (IT) arena in understanding their responsibilities, a summary of required security practices for users of unclassified information systems (IS) is provided as a Mandatory Reference. While this document is not all-inclusive, it does provide some fundamentals, which will help users implement improved IS security practices. (See Mandatory Reference, **Information System Security Rules of Behavior for All Computer Network (AIDNET) Users or "ISSO User Rules of Behavior"**)

545.3.3 Personnel Security Requirements for Access to Unclassified IS

Effective Date: 04/25/2002

Users must implement the following personnel security policies and associated procedures when processing unclassified data on information systems in Washington and at the Missions. (See **ADS 566, U.S. Direct-Hire and PASA/RSSA Personnel Security Program**, and **ADS 567, Classified Contracts, Grants, Cooperative Agreements, and Contractor/Recipient Personnel**, for more information on personnel security.)

Only individuals who meet the requirements for moderate risk automated data processing positions must be members of the systems group or users with special access privileges. (See **ADS 566** and **ADS 567**)

Program Managers and designated ISSOs, in coordination with the Office of Security, must ultimately ensure all personnel accessing USAID/W computer systems and networks have, at a minimum, an employment authorization prior to being granted access to any system or network owned or operated by USAID. (See **ADS 566** and **ADS 567**)

a. Required Access Procedures

No individual USAID employee, contractor, or other USAID IS user will be provided direct access to any USAID IS until the following procedures have been completed:

- Execution of the USAID Computer System Access & Termination Request, endorsed by a USAID direct-hire employee (See Mandatory Reference, **USAID Computer System Access and Termination Request, AID Form 545-4**);
- Completion of USAID-approved Information Security orientation/training;
- Execution of the USAID Unclassified Information Systems Access Request Acknowledgement, AID Form 545-1 (See Mandatory Reference, **USAID Unclassified Information Systems Access Request, AID Form 545-1**);
- Receipt by the user of the **Information System Security Rules of Behavior for All Computer Network (AIDNET) Users or "ISSO User Rules of Behavior"**; and
- If the user will be given unsupervised access to any USAID IS containing Sensitive But Unclassified data, the user and his or her supervisor must also execute the USAID Sensitive Data Nondisclosure Agreement. (See Mandatory Reference, **USAID Sensitive Data Nondisclosure Agreement, AID Form 545-5**)

b. Contracts

Program Managers and designated ISSOs must ensure no individual is awarded a contract, permitted to provide goods and/or services under a contract, or retained under a contract unless such an action is clearly consistent with the interests of USAID. No individual is permitted access to any USAID IS until

- A personnel security investigation or background check is completed at the level appropriate for the information to be accessed;
- It is determined that the individual's employment is clearly consistent with the interests of USAID goals and objectives;
- A favorable access eligibility determination is issued by the responsible Agency organization;
- The individual completes USAID-approved Information Security orientation/training and receives a copy of the Mandatory Reference, Information System Security Rules of Behavior for All Computer Network (AIDNET) Users or "ISSO User Rules of Behavior"; and
- The individual executes all necessary documentation, including the USAID Unclassified Information Systems Access Request Acknowledgement, AID Form 545-1.

c. Missions

All personnel accessing USAID Mission computer systems must ultimately have, at a minimum, a certificate of Acceptability for Employment prior to being granted access to any information system owned or operated by USAID. (See **ADS 566, Personnel Security Programs**, and **ADS 567, Classified Contracts, Grants, Cooperative Agreements, and Contractor/Recipient Personnel**) The Executive Officer (EXO) must ultimately request, in writing, the Regional Security Officer (RSO) to perform the highest level background investigation available within the host country on local vendor contract maintenance personnel. As a minimum, the interim procedures listed in subsection 545.3.3.a must be followed prior to permitting an individual initial access to any USAID IS.

545.3.4 Personnel Management

Effective Date: 08/01/2000

A statement specifying responsibilities for information systems security must be included in position descriptions and work requirements statements for IT Specialists/System Managers and members of the system staff having responsibility for programming, operating, or managing applications or systems. The Bureau for

Management, Office of Human Resources (M/HR) is available to assist USAID supervisors in developing position descriptions.

545.3.4.1 Separation of Duties

Effective Date: 04/25/2002

The Program Manager, designated ISSO, IT Specialist, or System Manager must structure user access privileges to reflect the separation of key duties implemented for functions supported by the application. All user access privileges must be consistent with the separation of duties established for manual processes and be reviewed on an annual basis. The security principle of "least privilege" should be employed whenever practical to minimize the access of system users to only the system functionality and data essential for their role.

545.3.4.2 Management of Personnel -- Computer Room/System Access, USAID/W

Effective Date: 08/01/2000

The Program Manager, designated ISSO, IT Specialist, or System Manager must revoke the user access privileges of people who no longer require system access or who have severed their relationship with the Agency. Such revocation must take place immediately upon the person's status change or departure.

The IT Specialist/System Manager must

a. Designate the room or office space that houses the central processing unit or server for a distributed system or local area network, and associated data storage devices, as a limited access area restricted to authorized personnel only;

b. Ensure that custodial and building maintenance personnel entering the computer room are under continual observation by personnel with authorized unescorted access; and

c. Limit physical access to the operating system and application software designated for use on the Agency's computer systems and networks to personnel identified on the Authorized Access List. (See Mandatory Reference, **Authorized Access List, AID Form 545-2**)

545.3.4.3 Management of Personnel -- Computer Room/System Access at Missions

Effective Date: 08/01/2000

EXOs/ISSOs must request the RSO to perform the highest level background investigation available at Missions on all foreign nationals and local contractors with special access privileges (e.g., backup operator privileges). EXOs/ISSOs must approve, in writing, all users of systems processing Sensitive But Unclassified (SBU) data. EXOs/ISSOs must request the Office of Security to perform background

investigations on U.S. citizen system staff and application users with special access privileges (e.g., operator privileges, or access to the computer room). EXOs/ISSOs must approve, in writing, all users of systems processing SBU data.

545.3.4.4 Documentation of Authorized Computer Room/System Access

Effective Date: 08/01/2000

a. Authorized Access List

The designated ISSO must develop and maintain a list of personnel authorized unescorted access into the computer room. The IT Specialist/System Manager must sign and post the "Authorized Access List" at all entrances to the computer room. The "Authorized Access List" must also prominently indicate personnel to be contacted in the event of an emergency. (See Mandatory Reference**, Authorized Access List, AID Form 545-2**)

b. Visitors Log

The IT Specialist/System Manager must maintain a visitors log for all persons entering the computer room who do not have unescorted access privileges. Only personnel listed on the "Authorized Access List" are authorized to escort visitors. Individuals not on the "Authorized Access List" must sign the visitors log prior to being allowed access into the computer room. While in the computer room, visitors must be under continuous visual observation by a person with authorized unescorted access. (See Mandatory References, **Authorized Access List, AID Form 545-2**, and **Visitors Log, AID Form 545-6**)

545.3.5 Technical Security

Effective Date: 06/27/2001

USAID Offices, Bureaus, and Missions must implement software and hardware controls to provide adequate protection for Agency information and system resources. Due to differences in hardware and software capabilities, Agency personnel must implement the following policies that are applicable to their specific system.

545.3.5.1 Hardware/Software Controls

Effective Date: 04/25/2002

a. The IT Specialist/System Manager must control access to specialized system software, utilities, and functionality that could be used to gain unauthorized access to application data and program code. The IT Specialist/System Manager must keep access to these resources to the minimum number of authorized users required to accomplish program objectives.

b. Users must not physically connect personally owned computer systems or communication devices (including laptops and pocket computers, network enabled cellular phones, and personal digital assistants (PDAs)) to U.S. Government-owned

systems or communication devices within USAID facilities. Note: The use of Agency-issued PDAs is addressed in section 545.3.5.8.

c. The IT Specialist/System Manager must equip stand-alone computer systems with security enhancement controls, (e.g., software products, or host dependent firmware products) only as approved, identified, or recommended by M/IRM.

d. Application Software

The IT Specialist/System Manager must ensure that only M/IRM/SDM-approved or -distributed versions of customized corporate application software are used on computer systems and networks owned or operated by USAID. A list of SDM-approved software is available on the USAID SDM/ILAB website at **http://ntrrbln03/Web/sdmpage.nsf/ILAB Sections?OpenPage**

Agency employees, other than authorized application developers, must not modify Agency standard application software.

Employees developing application software for Agency systems must develop and document their application software in accordance with M/IRM standards. (See Mandatory References, **ADS 543, Corporate Information Systems**, and **ADS 550, End-User Applications**)

The IT Specialist/System Manager must ensure that all new releases, upgrades, or patches to Agency operating system software and customized corporate application software installed on Agency systems have been approved and distributed by M/IRM/SDM. Software developed by or for Agency facilities or Missions must address application-specific security measures in all user guides, installation specifications, and backup and recovery operations.

Software applications transported between USAID offices and facilities must remain under Agency control during transport, or be sent by a contract courier service via diplomatic pouch or commercial contract courier service.

The IT Specialist/System Manager must implement all application controls to ensure that users are assigned access rights and privileges consistent with their functional responsibilities and authorities. Access rights and privileges must be based on need-to-know, separation of duties, and management authorization.

The IT Specialist/System Manager and designated ISSO must ensure that personally owned application software, shareware, and freeware are not installed on computer systems owned or operated by the Agency.

All software must be scanned for viruses and other malicious programming code prior to installation on any computer system or network owned or operated by the Agency. Data files created or used on systems or network equipment not owned and operated

by the Agency and locally purchased off-the-shelf software must be scanned for viruses and other malicious programming code prior to installation on any system or network owned or operated by the Agency.

545.3.5.2 Security Controls
Effective Date: 04/25/2002

The IT Specialist/System Manager must ensure that necessary security controls are implemented to prevent unauthorized access to USAID systems.

545.3.5.3 Workstation Restrictions
Effective Date: 06/27/2001

Within USAID-operated workspaces, IT Specialists/System Managers must restrict users to USAID workstations and printers within the user's immediate work area.

IT Specialists/System Managers must ensure that USAID systems automatically disconnect a logged-on workstation from the system after a predetermined period of inactivity.

IT Specialists/System Managers must limit unsuccessful logon attempts from any USAID workstation to three. After three unsuccessful logon attempts, the system must automatically lock out the workstation. Only the system staff must be given the capability to reset a workstation after lockout.

545.3.5.4 User-IDs
Effective Date: 04/25/2002

IT Specialists/System Managers must assign individual users a minimum three character user-ID. The user-ID must be unique to each user and must identify the user to the system. The assignment of more than one user-ID or a phantom user-ID is prohibited.

545.3.5.5 Password Controls
Effective Date: 04/25/2002

The following procedures apply to system passwords:

- Whenever possible, passwords must be user generated under the supervision of access control software. In facilities where access control software is not available, the IT Specialist/System Manager must create and distribute user passwords in a controlled manner, and in such a way that an audit trail record of password date and time of issuance, receipt, use, change, expiration, and termination is maintained.

- System users must gain access to USAID networks or distributed systems only after entering their unique user-ID and password.

- Passwords must be randomly selected. Passwords must not be easily guessable nor contain names or words in any dictionary. Passwords must consist of at least seven (7) characters and employ three of the following four character categories in a random pattern: uppercase letters, lowercase letters, numbers, and symbols. IT Specialists/System Managers or designated ISSOs may specify additional password requirements or restrictions as required to ensure the security of specific operating systems or applications.

- USAID passwords must be valid for a period of not more than 90 days or not more than 30 days if used for dial-in access.

- Upon reaching the maximum lifetime, the operating system or security software must prompt the user or IT Specialist/System Manager to change passwords.

- System users must not write their password(s) anywhere nor share their system passwords with anyone. (See Mandatory Reference, **Information System Security Rules of Behavior for All Computer Network (AIDNET) Users or "ISSO User Rules of Behavior"**)

- IT Specialists/System Managers must activate the audit trail capabilities provided by the operating system and security software installed on Agency systems.

- The IT Specialist/System Manager must manage the creation, use, and deletion of user-IDs and passwords to prevent unauthorized access to the system.

- The designated ISSO must ensure that all system users are aware of the private nature of their passwords. Users must inform the designated ISSO, Program Manager, Division Chief, or IT Specialist/System Manager if they suspect their password has been compromised. The designated ISSO must, in turn, work with the IT Specialist/System Manager to conduct an investigation and to make recommendations for action.

- Program Managers, Division Chiefs, or supervisory personnel at Missions must annually review the access privileges of each application user under their supervision to verify that system access privileges originally granted are still appropriate.

The IT Specialist/System Manager must not maintain permanent computer system user-IDs and passwords for visitors, vendor service, or training people. Also --

- The IT Specialist/System Manager must delete all default user-IDs and passwords supplied by the vendor during system manufacture and installation once installation is complete.

- The IT Specialist/System Manager must cause all system users to change their passwords under the following conditions:

  - At least every 90 days (30 days for dial-in access);

  - Immediately following any suspected compromise; and

  - Whenever there are changes in personnel with system security authority.

The IT Specialist/System Manager must immediately delete user-IDs and passwords whenever

- The Program Manager, Division Chief, or designated ISSO determines that the user no longer requires system access;

- The user terminates employment with the Agency or transfers to another office; or

- The user is the subject of a criminal or national security investigation.

The IT Specialist/System Manager must provide any outside auditors/reviewers with any application-specific information necessary to assist in any audit/review, and must retain written documentation of all directed changes.

545.3.5.6 Technical Security Controls

Effective Date: 06/27/2001

The IT Specialist/System Manager must ensure the following:

- All security software provided as part of the original system configuration (e.g., audit trail) is installed and operational.

- Each system user is assigned a valid and appropriate logon procedure to control the processing options available to the system user.

- Controls are implemented that limit access to files, programs, and data to users or groups of users with the same need-to-know. Need-to-know must be based on functional responsibilities, operational requirements, supervisory responsibilities, or a combination of these factors.

- Password file maintenance is restricted to the IT Specialist/System Manager. Passwords must be screen-suppressed during logon and re-authentication.

- Stand-alone computer systems must be equipped with security enhancement controls approved and/or identified by the ISSO for USAID. Such enhancements must include software products or host dependent firmware products.

545.3.5.7 Audit Trail

Effective Date: 04/25/2002

The audit trail must record at least the following events and any other events deemed appropriate by the Program Manager, EXO, designated ISSO, or M/IRM:

- Multiple logon failures;
- Logons during non-business hours;
- Program or file access denial;
- Addition, deletion, or modification of users or program access privileges; and
- Changes in file access restrictions.

IT Specialists/System Managers must archive the audit trail to a file with the most stringent access restrictions available. Audit trails containing financial information and transactions must be retained for a period of two years. Audit trails containing information not related to financial information and transactions must be retained for a period of six months.

545.3.5.8 Personal Digital Assistants (PDAs)

Effective Date: 06/27/2001

Guidance on the use of USAID-issued personal digital assistants (PDAs) in conjunction with USAID systems and networks follows:

a. Although a PDA often is used as an independent "information system," these devices also can be set up to synchronize data with standard computer terminals. Users must not physically connect personally owned PDAs to USAID-owned systems or communication devices within USAID facilities. If USAID issues you a PDA and you need to connect the USAID PDA to other USAID equipment, make sure all configuration management requirements and essential security procedures are followed.

b. Commercial Internet service providers (ISPs) of e-mail services may not follow all essential IS security practices. Using a USAID-issued PDA in conjunction with commercial ISPs can pose a high operational risk, and may allow unauthorized collection of sensitive information.

c. Individuals may use USAID-issued PDAs (and appropriate related software applications) to

- Process unclassified information from desktop workstations. This would include updating typical PDA features such as schedules, contact information, notes, e-mail, and other PDA data items.

- Take notes, save information, or write e-mails when away from desktop workstations, whether down the hall or out of the country.

- Synchronize information with desktop workstations.

d. DO NOT USE USAID-issued PDAs for any of the following actions:

- Do not process or maintain classified information on PDAs. There are currently no approved methods for clearing (sanitizing) classified information from these devices. If a PDA becomes "contaminated" with classified data, the user must turn the USAID-issued PDA over to the Office of Security.

- Do not synchronize information across a network using a wireless connection. The configuration required to permit this functionality introduces unacceptable risks into a network -- opening firewall ports and sending passwords in the clear. Exceptions to this restriction will be evaluated on a case-by-case basis and require written approval from the ISSO for USAID.

e. USAID software security restrictions apply to these devices. Also, the only authorized connection through a PDA modem is to an official USAID remote access server (RAS) account protected by an authorized network control center firewall. Do not synchronize a PDA remotely by direct dial-in access to USAID desktops.

f. Users will not be issued a USAID PDA until they agree to follow all the policy guidance outlined in subsection **545.3.5.8**.

545.3.6 Administrative Security

Effective Date: 06/27/2001

Access to information systems must be restricted to individuals who require access to perform their official duties. The level of access granted must limit users to only the information needed to complete assigned responsibilities. The following policies must be followed to administer and document system access controls.

545.3.6.1 ISSO and Alternate ISSO

Effective Date: 04/25/2002

a. Appointment of ISSOs and Alternate ISSOs -- M/IRM must designate, in writing, an Agency employee within IRM to serve as the ISSO for USAID/W general support

systems. The designee must have a TOP SECRET security clearance and be a U.S. citizen direct-hire employee.

b. Program Managers must designate, in writing, an ISSO and alternate ISSO to manage the information systems security program for their organizational entity in USAID/W. Alternates must fulfill the designated ISSO's duties when the ISSO is absent. This requirement applies regardless of the size or number of systems. Both designees must be U.S. citizen employees and have at least a SECRET security clearance. Copies of the written appointments must be provided to designee ISSOs and the ISSO for USAID, with the original retained in the central system file. Program Managers and designated ISSOs must make periodic checks of system hardware and/or software to ensure full compliance with this provision and other Federal information security laws and regulations. The designated ISSO at USAID Missions is usually the EXO; however, a Mission Director may appoint another U.S. citizen with a SECRET clearance as designated ISSO instead.

545.3.6.2 Systems Access Controls

Effective Date: 04/25/2002

The IT Specialist/System Manager manages, administers, controls, and limits computer system access to individuals requiring system access in the performance of their official duties. The IT Specialist/System Manager must limit the access of system users to the minimum level necessary to perform their official duties.

a. USAID Computer System Access & Termination Request Form

IT Specialists/System Managers, Program Managers/supervisory management personnel, or EXOs/ISSOs must complete a USAID Computer System Access & Termination Request form for each staff member requiring interactive system access. (See Mandatory Reference, **USAID Computer System Access & Termination Request, AID Form 545-4**)

The IT Specialist/System Manager must sign all USAID Computer System Access and Termination Request forms after reviewing each form for accuracy and technical anomalies, and retain completed forms in central files for at least six months. For details on USAID's records management program, see ADS 502, The USAID Records Management Program. (See Mandatory Reference, **ADS 502**)

The Computer System Access & Termination Request form (AID 545-4) must include the user's name, the applications the user is authorized to access, and the type of access required within each application. Whenever a user's functional responsibilities change, a new system access request form must be completed by the Program Manager, Division Chief, or EXO/ISSO.

Program Managers, Division Chiefs, or EXOs/ISSOs are responsible for authenticating and verifying the information systems access requirements for each user under their supervision. The IT Specialist/ System Manager must provide assistance, as

necessary, in completing the USAID Computer System Access & Termination Request form.

Program Managers (USAID/W) or EXOs/ISSOs must determine who within their organization requires access to computer systems approved to process SBU information. This determination must be indicated on the USAID Computer System Access & Termination Request form. (See Mandatory Reference**, AID Form 545-4**)

In USAID/W, IT Specialists must immediately terminate user system access upon written notification by the user's Program Manager or Division Chief.

At Mission locations, the System Manager must immediately terminate user system access upon written notification by the EXO/ISSO.

Managers and Division Chiefs must provide the designated ISSO with written notification of a user's system termination no later than one working day after the user no longer requires system access. The designated ISSO must forward the written notice to the IT Specialist for action. The IT Specialist must retain user system termination notifications in the central system file for at least six months after the date of the user's removal from the system.

The EXO/ISSO must provide the System Manager with written notification of a user's system termination no later than one working day after the user no longer requires system access. The System Manager must retain user system termination notifications in the system's central file for at least six months after the date of the user's removal from the system.

b. Training

Prior to gaining access to any of the Agency's computer systems or networks, each user must complete USAID-approved computer security awareness training and agree to abide by all Agency computer security policies, procedures, and guidelines in the USAID Automated Directives System (ADS) and the ADS 545 Mandatory Reference, **Information System Security Rules of Behavior for All Computer Network (AIDNET) Users or "ISSO User Rules of Behavior"**. All new users must complete a form AID 545-1, **Unclassified Information Systems Access Request Acknowledgement**.

545.3.6.3 Use of Systems

Effective Date: 04/25/2002

People with access to computer systems owned or operated by USAID must ensure the protection of information, equipment, and facilities. All managers and employees must with guidance in this ADS Chapter and its Mandatory References. In addition, non-compliance (to include information systems security incidents, abuse, or misuse) must be reported to the appropriate supervisor.

Supervisors must take appropriate administrative or punitive action, after consultation with the Bureau for Management, Office of Human Resources (M/HR) and/or the General Counsel (GC). If the offending user is a contractor, coordination with the Bureau for Management, Office of Procurement (M/OP) usually will also be necessary. Based on the nature of the security lapse, it may be appropriate to terminate an individual's access to USAID networked IT systems until remedial ISS training has been completed. Details on authorized use(s) of USAID IS can be found in ADS 541, Information Management. (See Mandatory Reference, **ADS 541**) Violations of this section must be enforced in accordance with ADS 568, National Security Information and Counterintelligence Security Program. (See Mandatory Reference, **ADS 568**)

Use of information systems equipment owned or operated by the Agency for purposes other than official U.S. Government business or authorized purposes is prohibited. For details on "limited personal use" see **ADS 541** and its related reference, Recommended Executive Branch Model Policy/Guidance on "Limited Personal Use" of Government Office Equipment Including Information Technology.

Unattended workstations must not be left unsecured while applications and/or sensitive files are open and/or accessible. The designated ISSO must instruct all system users that activities occurring when a workstation is left logged-on are the responsibility of the user.

a. Labels

Labels indicating the highest sensitivity level of information approved for processing on the system must be affixed to computer devices and removable media.

- The designated ISSO must ensure that each device associated with a computer system approved to process, store, or print SBU information is prominently labeled to indicate the level of processing authorized.

- In addition to displaying the highest level of information approved for processing on the system, the device label must also indicate the name and office phone number of the designated ISSO responsible for the security of that piece of equipment.

- The IT Specialist/System Manager must label all removable magnetic media to indicate the highest level of information approved for processing on the system.

- Users are responsible for affixing labels to removable media (i.e., floppy disks) indicating whether sensitive information is stored on that media.

b. After-Hours System Operation

The designated ISSO and IT Specialist/System Manager must ensure that appropriate after-hours restrictions are developed and implemented for each of their systems. The

System Manager/IT Specialist must ensure that all system logs in effect during normal operations are also activated during after-hours operations.

545.3.6.4 Classified Information

Effective Date: 06/27/2001

Classified information must only be entered onto a system approved for processing such information. The creation, processing, or storage of classified information on systems not approved for such purposes is a security violation as defined in ADS 568, National Security Information and Counterintelligence Security Program. The limitations against retroactively classifying data also apply to documents prepared on Agency information system equipment. (See Mandatory Reference, **ADS 568**)

The requirements for processing classified national security information overseas are contained in 12 FAH-6 (12 Foreign Affairs Handbook-6, OSPB Security Standards and Policy Handbook).

No classified information processing will be authorized at an overseas Mission without the approval of the Office of Security (SEC) and M/IRM. (See also **ADS 552, Classified Information Systems Security**, for details on security requirements for processing classified data on USAID equipment within the United States; **ADS 562, Physical Security Programs (Overseas);** and **ADS 568, National Security Information and Counterintelligence Security Program**)

545.3.6.5 Sensitive But Unclassified (SBU) Data

Effective Date: 04/25/2002

Sensitive But Unclassified data is information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The designated ISSO must advise all system users to employ the most stringent access controls available (e.g., using password protection, or processing files on a floppy disk using a stand-alone microcomputer) when processing SBU information or any information concerning an individual that is legally protected, compromising, adverse, embarrassing, or derogatory.

Storage of such information on distributed or networked systems must be minimized.

More details on sensitive data can be found in the following Mandatory References:

- **Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources;**
- **Appendix III, OMB Circular A-130, Security of Federal Automated Information Systems**;
- **12 FAM 090, Definitions of Diplomatic Security Terms;**

- **ADS 507, Freedom of Information Act (FOIA);**
- **ADS 508, Privacy Act**; and
- **ADS 509, Creating, Altering, or Terminating a System of Records (Records Pertaining to Individuals)**.

Some examples of SBU data follow:

- Testing and evaluation materials;
- Records specifically exempted from disclosure by statute;
- Proprietary commercial data;
- Deliberative process (policy development) materials;
- Legally privileged materials; and
- Law enforcement and/or investigation files.

Users must not enter or store medical information protected under the Privacy Act of 1974 on any distributed or networked system. Gathering, processing, storing, distributing, and safeguarding medically privileged information is a function reserved for the U.S. Department of State, Medical Services.

Sensitive But Unclassified (SBU) Processing

- Users must process SBU information on unclassified computer systems under conditions approved by the designated ISSO, in coordination with the ISSO for USAID.
- E-mail messages or attachments containing SBU information must never be sent or forwarded to unauthorized recipients; consider using means other than e-mail to transmit SBU information. All those entrusted by the Agency with SBU information must safeguard it. Reasonable security measures must be implemented to ensure access to SBU information is restricted to authorized users or groups on the basis of a clearly demonstrated need to know or use. Encryption methodologies approved by the Agency ISSO must be used when transmitting SBU information over the Internet.
- SBU access must be based on need-to-know and permitted only after individuals are granted a favorable background investigation. The Office of Security conducts background investigations for U.S. citizens and legal resident aliens, and the Regional Security Officer (RSO) conducts background investigations for foreign nationals overseas.

- SBU information must never be processed or stored in public directories. Whenever possible, SBU information must be stored off line (e.g., on floppy disks and/or removable hard drives).

- During non-duty hours, SBU information must be secured within a locked room or secured in a locked container. (See Mandatory Reference, **ADS 562, Physical Security Program (Overseas)**)

- Printed materials and removable media containing SBU information must be marked sensitive or carry a distribution restriction alerting data owners and recipients of the additional protective measures required.

- Information systems must be certified to process, store, and print SBU information. System users must not originate, process, print, or store SBU information on computer systems not formally approved for that purpose.

- Before users and uncleared vendor maintenance personnel are allowed unsupervised access to a computer system approved to process SBU information, a favorable background check or U.S. Government-granted security clearance must be validated by the designated ISSO.

545.3.6.6 Protection of Media and Output

Effective Date: 06/27/2001

The IT Specialist/System Manager must store back-up copies of operating system and application software in a locked area or approved security container (available through the Bureau for Management, Office of Administrative Services, Consolidated Property Division (M/AS/CPD)). The designated ISSO must review and approve all facility-specific procedures for transportation and control of electronic media. System users must ensure that reports containing SBU information are appropriately secured in a manner commensurate with the magnitude of loss or harm that could result from unauthorized disclosure. Non-sensitive media under the control of system users (i.e., floppy disks) do not have to be secured during working hours but must be stored out of view after hours. Media containing SBU information must be stored as directed in 12 FAM 540. (See Mandatory Reference, **12 FAM 540**) All media must remain under the control of cleared Agency or contractor employees during transport or be shipped via registered U.S. Mail.

545.3.6.7 Monitoring System Users

Effective Date: 06/27/2001

The designated ISSO must conduct reviews of randomly selected user word processing documents, files, and floppy disks on a monthly basis to ensure that users are adequately protecting SBU information; archiving SBU information; maintaining SBU information on the system for the minimum amount of time; and not processing classified information on the system.

545.3.6.8 Security Incident Reporting

Effective Date: 06/28/2002

Recent Federal legislation and regulatory guidance stress the importance of incident response in protecting information systems (IS). Should an incident occur, a prompt, coordinated response could limit damage, speed recovery, and help restore service to users.

An information security incident is an occurrence having actual or potentially harmful effects on an IS. The types of activity widely recognized as harmful include, but are not limited to, the following:

a. Attempts (either failed or successful) to gain unauthorized access to (or use of) a system or its data;

b. Unwanted disruption or denial of service;

c. Unauthorized changes to system hardware, firmware, or software, including adding malicious code (such as viruses); or

d. Detection of symptoms of the above, such as altered or damaged files, virus infection messages appearing during start-up, inability to log in, etc.

The following steps must be taken when a security incident is suspected:

a. System users discovering or suspecting incidents (e.g., altered or damaged files, messages appearing during startup, inability to log in, etc.) must immediately report such incidents to their supervisor.

b. The user's supervisor must determine if a security incident may have occurred and then report the suspected incident to the IT Specialist (USAID/W) or System Manager (Missions).

c. The IT Specialist/System Manager must document, in a system operation log, all security-related abnormal system operations such as unexplained changes in user or program access privileges, improper system responses to access control processes, or other hardware or software failures that result in unauthorized disclosure, data loss, or modification of system programs or data. Upon determining that an incident has occurred, the System Manager/IT Specialist must immediately notify the designated ISSO and the USAID Help Desk.

d. The Help Desk must notify the ISSO for USAID of the incident and maintain a record of the activity.

e. The ISSO for USAID must coordinate the resolution of the incident and ensure appropriate senior USAID officials and Federal organizations are notified.

(NOTE: Additional details on Agency Incident Response responsibilities are contained in the Mandatory References, **Incident Response Guidance for Unclassified Information Systems** and **Information System Security Rules of Behavior for All Computer Network (AIDNET) Users or "ISSO User Rules of Behavior"**.)

545.3.6.9 Disposal of Sensitive Media, Output, and Equipment

Effective Date: 04/25/2002

System users must destroy sensitive reports by burning, shredding, or another designated ISSO-approved method when they are no longer needed.

Sensitive magnetic storage media used on Agency systems must be overwritten using overwrite procedures approved by the ISSO for USAID or degaussed with a magnet approved by the ISSO for USAID.

- The IT Specialist/System Manager and designated ISSO must ensure that sensitive magnetic storage media used on Agency systems are not removed from U.S. Government-controlled premises for maintenance, credit, or sale unless all information on the media has been sanitized.

- If a fixed disk (e.g., fixed disk, disk cartridge, or disk pack) cannot be returned to the vendor for credit, the IT Specialist/System Manager must ensure that appropriate security procedures are followed when returning the damaged disk to M/IRM for destruction.

- The IT Specialist/System Manager must destroy other types of damaged, sensitive magnetic media (i.e., floppy disks and tapes) by burning, shredding, or using other methods approved by M/IRM (USAID/W) or the RSO of the host embassy or consulate.

In order to follow contractual procedures for returning damaged fixed disks to the vendor for credit, the IT Specialist/System Manager must contact M/IRM for appropriate vendor-specific procedures. The following actions are required when returning damaged disks to M/IRM for destruction:

- Disassemble, hand-carry, or send the disks to the ISSO for USAID via registered U.S. Mail (USAID/W) or unclassified diplomatic pouch (Missions). If disassembly tools are not available, sealed removable hard disks must be shipped intact. Packages must be marked "For Destruction."

- For SBU disk packs only, the disk packs must be degaussed and the packages sent to the ISSO for USAID marked with the appropriate

classification. Approved degaussers for sanitizing SBU media prior to shipment are obtainable by contacting the ISSO for USAID (USAID/W), or at the Missions, the RSO of the host embassy or consulate.

545.3.6.10 Violations

Effective Date: 06/27/2001

The designated ISSO must randomly review selected files, documents, and storage media associated with information systems under the designated ISSO's purview to ensure that users are not processing classified information on equipment not approved for this purpose. All violations noted in these reviews must be reported and processed in accordance with the guidance set forth in ADS 568, National Security Information and Counterintelligence Security Program. (See Mandatory Reference, **ADS 568**)

System users must not originate, process, print, or store classified information on any computer system not approved for that purpose. Individuals violating this provision must be subject to the security violation procedures set forth in ADS 568, National Security Information and Counterintelligence Security Program. System users must not originate, process, print, or store SBU information on computer systems not formally approved for that purpose. Passwords to unclassified systems and sensitive data must be afforded a degree of protection commensurate with the magnitude of harm or loss that could result from inadvertent or deliberate disclosure. Employees disclosing passwords to unclassified systems are subject to administrative sanctions or disciplinary actions. Program Managers, designated ISSOs, and EXO/ISSOs must take appropriate action to ensure that all USAID personnel, contractors, and vendors meet security requirements for unclassified computer systems.

Unauthorized disclosure of SBU information may result in criminal and/or civil penalties. Supervisors may take disciplinary action, as appropriate.

The Program Manager or EXO/ISSO is authorized to impose administrative sanctions or disciplinary actions for failure to comply with these regulations (except those incidents related to classified material). The designated ISSO must investigate all known or suspected incidents of noncompliance and inform the Program Manager or Mission Director of the results of those investigations.

545.3.6.11 System Maintenance

Effective Date: 06/27/2001

The IT Specialist/System Manager or an appropriate designee must monitor vendor maintenance personnel when they are accessing system equipment. The IT Specialist/System Manager must maintain a log of all maintenance or service performed on the system, and ensure that maintenance personnel do not remove any magnetic media from Agency facilities until it has been sanitized via degaussing or overwriting. The IT Specialist/System Manager must prohibit maintenance personnel from running remote diagnostics on any USAID computer system from an off-site location not approved by the ISSO for USAID and the Telecommunications and Computer

Operations (M/IRM/TCO) Division. The maintenance log must include the date of service, service performed, hardware or software involved, personnel performing the service, equipment removed or replaced, and system condition or status following the service. Records must be retained for a period of six months after the date of entry in the central system file.

545.3.6.12 Record Keeping

Effective Date: 06/27/2001

Within each USAID organization, the designated ISSO and IT Specialist/System Manager must ensure that all original documents, logs, and records are maintained, after processing, in a central system file for each computer system their organization is operating. For details on USAID's records management program, see **ADS 502**. The following documents, logs, and records must be maintained:

- USAID Computer System Access & Termination Requests (**AID Form 545-4**);
- USAID Unclassified Information Systems Access Request Acknowledgement (**AID Form 545-1**);
- USAID Sensitive Data Nondisclosure Agreement (**AID Form 545-5**);
- Contingency Operation, Disaster Recovery, and Emergency Action Plans;
- Copies of Waivers or Exceptions;
- Copy of the most current Authorized Access List (**AID Form 545-2**);
- System Certification;
- Security Reviews;
- Designated ISSO and Alternate ISSO Appointment Documentation;
- Annual Compliance Review (**AID Form 545-3**);
- System Operation and Maintenance Logs;
- Computer Room Visitors Log (**AID Form 545-6**); and
- System Inventory.

The IT Specialist/System Manager must retain all audit trail files and records for a period of six months. USAID Sensitive Data Nondisclosure Agreements and USAID Unclassified Information Systems Access Request Acknowledgements will be destroyed

when the user to whom the forms relate terminates his or her USAID employment, when no longer applicable, or when superseded.

545.3.6.13 Security Reviews

Effective Date: 06/27/2001

Each security review must address personnel, administrative, technical, and physical security practices. (See Mandatory Reference, **Unclassified Information Compliance Review, AID Form 545-3**) The results of the review must be retained in the central system file with a copy forwarded to the ISSO for USAID.

a. Security evaluations must address the Program Manager's Office or Mission's compliance with applicable Federal and Agency information systems security policies, standards, and requirements. Each evaluation must result in a draft report delineating the findings and recommendations of the ISSO for USAID. The Program Manager or EXO/ISSO must provide written comment on the draft report within 30 calendar days.

b. The final report must delineate the findings and recommendations of the ISSO for USAID, incorporate the Program Manager's or EXO/ISSO's comments, and be distributed to the Program Manager or EXO/ISSO, M/IRM, and the Office of Security. The results of an information systems security evaluation, which may identify USAID vulnerabilities, must be appropriately marked for those with a need-to-know (e.g., banner the top of each page "Release Restricted--Verify Need-to-Know Before Permitting Access") in addition to other administrative markings (such as SBU, Not Releasable to Foreign Nationals, etc.) appropriate to the content of the document.

c. Audit trail reviews must assess potential security-related incidents such as the following: multiple logon failures; logons for after-hours use; addition, deletion, or modification of user or program access privileges; and changes in file access restrictions. The designated ISSO selects additional activities for review based on Office or Mission location and type of information processed.

d. The designated ISSO, in conjunction with the Program Manager or other appropriate Agency personnel, must conduct an annual review of user and system operation practices to evaluate compliance with this chapter. If, after review, it is determined that a security compromise occurred, then the reporting and investigation procedures delineated in ADS 568, Information and Counterintelligence Security Program, must be followed. (See Mandatory Reference, **ADS 568**)

e. The ISSO for USAID is authorized to conduct or direct the conduct of periodic security evaluations of information systems supporting the Agency.

f. The IT Specialist/System Manager or designated ISSO must generate and review the audit trail of all distributed systems at least monthly. The designated ISSO must review with the Program Manager and IT Specialist/System Manager all security-related anomalies discovered during audit trail reviews.

545.3.6.14 Training
Effective Date: 04/25/2002

The ISSO for USAID must provide initial and periodic/recurring system security awareness training to designated ISSOs, Program Managers, and users in USAID. Other Agency employees having security responsibilities for Agency computer systems and networks are encouraged to request special training. The designated ISSO must ensure that all personnel with access to systems and networks approved to process SBU information receive initial and periodic/recurring system security awareness training.

545.3.7 System Operation Requirements -- Logs, Certification, Backup, Emergency Actions, and Contingency Operation Planning
Effective Date: 08/01/2000

545.3.7.1 Logs
Effective Date: 08/01/2000

The IT Specialist/System Manager must ensure that a system operation log is maintained for all information systems operating under his or her authority. The system operation log must contain a record of all normal daily operations, system power-ups and power-downs, media mounts and dismounts, backup and recovery operations, and general environmental conditions. Installation, removal, or modification of system or application software must be noted in the log. Any unusual events or operating conditions must also be noted in the log. Logs must be maintained in the central system file for a minimum of six months from the date of the last entry.

545.3.7.2 System Certification
Effective Date: 08/01/2000

All information systems owned or operated by USAID in support of the Agency must be certified to operate. USAID computer systems that do not process classified or SBU information and that operate only in a stand-alone mode are exempt from this requirement. Voluntary certification of unclassified/non-SBU systems is authorized.

The ISSO for USAID must assist the requesting Bureau, Office, or Mission in the completion, coordination, and dissemination of all required analyses, documents, forms, and processes associated with the certification of information systems. (See Mandatory Reference, **Information System Certification and Accreditation Process, Approval to Operate**)

The Office of Security, in coordination with the RSO where appropriate, must assist the requesting Bureau, Office, or Mission in determining and installing appropriate physical security controls. (See **ADS 562, Physical Security Programs (Overseas),** and **ADS 565, Physical Security Programs (Domestic)**)

National-level guidance on the certification and accreditation process is contained in the Mandatory Reference **"National Information Assurance Certification and Accreditation Process** (NIACAP, National Security Telecommunications and Information Systems Security Instruction {NSTISSI} No. 1000)".

545.3.7.3 Backup

Effective Date: 08/01/2000

The IT Specialist/System Manager must implement and document backup procedures for system programs and information to ensure continuity of operations.

M/IRM/TCO, in consultation with the appropriate Program Managers, must identify and secure, through a contractual agreement, facilities to store backup media to ensure continuity of operations for systems operating in USAID/W. Such facilities must be off-site and employ appropriate environmental controls and alarm systems.

Wherever possible the storage location must be in a U.S. Government facility that is separate from the building housing the system. The System Manager is authorized to use a secure on-site alternate storage location if a suitable separate location is unavailable. Any on-site location must be as far away from the information processing facility as feasible. The System Manager must ensure that alternate storage locations are protected from extreme heat, humidity, and air pollution.

Backups must be securely stored on-site but as far away from the central processing unit as feasible. For USAID/W, off-site storage must be used for all backup files that are older than seven working days.

At Mission locations, the System Manager, in consultation with the EXO/ISSO, must identify a secure location to store backup media to ensure continuity of operations for all systems and network connections under the System Manager's purview.

The IT Specialist/System Manager must develop a system-specific schedule and procedure for backing up magnetic media (floppy disks for stand-alone computer systems excluded) used on central processors.

545.3.7.4 Emergency Actions

Effective Date: 08/01/2000

The IT Specialist/System Manager must develop emergency system power-down procedures to be instituted in the event of general building emergencies. Emergency system power-down procedures must be specified for all systems under the purview of the IT Specialist/System Manager. Each member of the system staff and the designated ISSO must receive training from the IT Specialist/System Manager in the implementation of these procedures and then be afforded opportunities to periodically practice the procedures.

545.3.7.5 Contingency Operation Planning
Effective Date: 08/01/2000

The IT Specialist/System Manager and designated ISSO must develop emergency action plans for each facility accommodating computer systems they operate in USAID/W. Such plans must be coordinated with the ISSO for USAID and be consistent with applicable Agency and local government emergency action plans. (See Additional Help item, **Contingency Planning for Information Resources**)

The IT Specialist/System Manager and designated ISSO at a Mission must develop site-specific emergency action plans. (See Additional Help item, **Contingency Planning for Information Resources**) The designated ISSO must retain copies of the most recent contingency operation, disaster recovery, and emergency action plans in the central system file; in the off-site backup storage facility and with the Executive Management staff representative (USAID/W); and in the backup media storage location and with the RSO (Missions).

The IT Specialist/System Manager and designated ISSO must review, update (if necessary), and test all emergency action plans annually, or when significant modifications are made to system hardware, software, or system personnel.

The ISSO for USAID must develop site-specific contingency operation and disaster recovery plans based on threat identification information and system asset accounting and valuation data provided to the ISSO for USAID by the IT Specialist/System Manager and designated ISSO. (See Additional Help item, **Contingency Planning for Information Resources**)

Users must protect data processed in the stand-alone mode by making periodic backups of all program files and data.

545.3.8 Physical Security
Effective Date: 04/25/2002

Responsible personnel must adhere to the following policies to ensure that systems approved to process SBU information are afforded the physical protection required for that level of data:

a. A computer system must only be approved to process SBU information if the facility housing the system is authorized to store SBU information and meets the standards established in **ADS 562, Physical Security Program (Overseas)**, and **ADS 565, Physical Security Programs (Domestic)**.

b. If a compromise of SBU information is suspected, the equipment, media, or document is to be immediately secured, and the ISSO for USAID and Program Manager or EXO/ISSO orally notified as soon as feasible. Written notification of the SBU compromise must be forwarded to these offices within two working days

of discovery. The Program Manager or EXO/ISSO must arrange to provide counseling and computer security awareness training for the offending user. If the Program Manager and/or designated ISSO determine an investigation is warranted, the designated ISSO must notify the Office of Security through the ISSO for USAID.

c. The designated ISSO, under the direction of the RSO at the Mission, must conduct or direct the conduct of an end-of-day security check of all work areas housing information systems approved to process, store, or print SBU information.

d. The IT Specialist/System Manager and designated ISSO must maintain a complete and up-to-date inventory of all system components and peripherals and their location. The inventory must be updated each time equipment is added to or removed from the system, and must be retained in the central system file.

e. People are prohibited from removing U.S. Government computer systems or media from Agency premises without the prior written approval of the designated ISSO and Executive Management staff representative.

f. Computer systems with removable media need not be located in locked offices; however, the designated ISSO must instruct users to appropriately secure removable media when not in use.

g. People must ensure that laptop computers either remain within view at all times or are appropriately secured. Laptop computers are not to be checked as luggage on public transportation and are not to be used to process classified or SBU information while in transit.

h. Sensitive media, output, and equipment must be disposed of in accordance with section 545.3.6.9, Disposal of Sensitive Media, Output, and Equipment.

545.3.9 Host Facility System Security Standards

Effective Date: 04/25/2002

The following policies apply when SBU processing is performed either at Agency facilities by non-Agency personnel or when Agency personnel must process SBU information at other U.S. Government facilities, or on systems managed by organizations outside USAID:

a. When Agency facilities, organizations, personnel, or contractors are hosting U.S. cleared personnel not associated with USAID and SBU processing is required, the computer security policies and procedures of USAID must take precedence.

If the other agency's policies and procedures are more or less stringent than those of USAID, then the policies of USAID must prevail until a senior representative of the other agency coordinates a resolution with USAID.

b. When personnel representing USAID are processing SBU information in U.S. Government facilities not operating under the auspices of USAID, or on systems managed by organizations outside USAID, the computer security policies and procedures of the host department or agency must take precedence.

If the computer security policies and procedures of the host department or Agency do not meet or exceed the computer security policies and procedures of USAID, then the computer security policies of the host must prevail until the senior USAID executive present, or designated representative, coordinates a resolution with the host department or Agency.

545.3.10 Special Considerations for Missions Operating in Critical Technical and Critical Human Intelligence Threat Environments

Effective Date: 12/22/1995

Missions located in geographic areas bearing a critical technical and critical human intelligence threat designation (available from the Office of Security and ISSO for USAID on a need-to-know basis) must operate information systems approved to process SBU information according to the following guidance:

a. System Access

(1) Agency personnel requiring access to system supervisory functions must be U.S. citizens with at least a SECRET clearance.

(2) Foreign nationals must be directly supervised by a U.S. citizen with at least a SECRET clearance during after-hours system use.

b. Technical Security

Certain policies and procedures for system connectivity are designated as SBU and CONFIDENTIAL information. Therefore, they are not provided in this chapter. Location-specific policies and procedures for system connectivity are available from the EXO/ISSO, RSO, or ISSO for USAID.

c. System Software

(1) System and application software must not be locally procured.

(2) Maintenance contractors and vendors must not use software that has been out of U.S. Government control unless it has been reviewed and approved by the ISSO for USAID.

(3) Foreign nationals are not permitted to program or modify system or application software used in conjunction with distributed or networked systems.

(4) The EXO/ISSO must destroy all damaged or otherwise unusable floppy disks and tapes in accordance with approved local media destruction procedures determined by the RSO.

545.3.11 Facsimile Equipment and Transmissions

Effective Date: 12/22/1995

Facsimile equipment that processes and transmits unclassified data is especially vulnerable to monitoring. Therefore, to minimize the impact of potential exposure of U.S. Government information to unauthorized persons, Agency organizations sending and receiving facsimile transmissions must adhere to the guidance in this section.

545.3.11.1 Procurement of Facsimile Equipment

Effective Date: 12/22/1995

The following guidance must be adhered to when purchasing facsimile equipment in USAID/W and at Missions:

a. Procurement procedures specified by the Bureau for Management, Office of Administrative Services (M/AS) and/or M/IRM must be used to purchase non-secure facsimile equipment and materials intended for use in USAID/W facilities.

b. Local procurement procedures must be used to purchase non-secure facsimile equipment and materials on an off-the-shelf basis (i.e., no special orders) at USAID Missions.

c. All newly purchased facsimile equipment must contain internal audit trail capabilities.

545.3.11.2 Installation and Repair of Facsimile Equipment

Effective Date: 12/22/1995

The following policies must be adhered to when facsimile equipment is installed or repaired in USAID/W and at Missions:

a. The designated ISSO must approve the location and installation of all facsimile equipment.

b. The Program Manager, designated ISSO, and/or Executive Management employees are authorized to permit supervised local service vendors to install and repair non-secure facsimile equipment.

c. The designated ISSO must ensure that a log is maintained of all maintenance or service performed on facsimile equipment. The log must be maintained by the designated ISSO in a central file.

545.3.11.3 Facsimile Transmissions

Effective Date: 01/12/2000

The following policies must be adhered to when transmitting or receiving information via facsimile equipment owned or operated by USAID:

a. Authorized Transmissions

(1) The designated ISSO must notify all facsimile users that Agency facsimile equipment is to be used only for official business or for authorized uses. Designated ISSOs are authorized to make periodic audits to ensure full compliance with this provision and other Federal information security laws and regulations.

(2) Users must transmit only unclassified, non-sensitive, non-record data via non-secure facsimile equipment.

(3) SBU information must be transmitted in compliance with 12 FAM 540. (See Mandatory Reference, **12 FAM 540**)

b. Unauthorized Transmissions

(1) The transmission of classified material over non-secure facsimile equipment is a security violation. Such violations must be handled in accordance with ADS 568, National Security Information and Counterintelligence Security Program, at USAID/W or 12 FAM 550 at USAID Missions. (See Mandatory References, **12 FAM 550** and **ADS 568**)

(2) The transmission of SBU data over non-secure facsimile equipment using unencrypted communication lines must be in accordance with 12 FAM 544 and 545. Employees transmitting SBU data using unauthorized facsimile equipment are potentially subject to sanctions, disciplinary actions, and/or civil and criminal penalties**.** (See Mandatory References, **12 FAM 544**, **12 FAM 545**, and **ADS 549, Telecommunications Management**)

(3) Any facsimile user or facsimile recipient discovering or suspecting unauthorized disclosure of information, unauthorized transmission of data, or unauthorized facsimile use must immediately report such incidents to the designated ISSO. At USAID/W, the designated ISSO in cooperation with the ISSO for USAID must initiate investigative actions. The

EXO/ISSO at overseas organizations, in coordination with the Office of Security, must initiate and/or coordinate appropriate investigative actions.

545.3.11.4 Administrative Management for Facsimile Equipment

Effective Date: 01/12/2000

The following administrative requirements must be implemented for facsimile equipment owned or operated by USAID:

a. Labeling

(1) The designated ISSO must ensure that all non-secure facsimile equipment is clearly labeled, "EQUIPMENT IS AUTHORIZED FOR TRANSMISSION OF NON-SENSITIVE UNCLASSIFIED INFORMATION ONLY."

(2) The designated ISSO must ensure that facsimile equipment authorized to transmit sensitive data is clearly labeled, "AUTHORIZED FOR THE TRANSMISSION OF SENSITIVE BUT UNCLASSIFIED INFORMATION."

(3) The designated ISSO must ensure that the security requirements associated with non-sensitive unclassified facsimile transmissions are prominently posted near all functioning non-secure facsimile equipment.

(4) Users are responsible for ensuring that each outgoing facsimile transmission clearly indicates the classification level, date and time of transmission, subject of the document, number of pages, and the sender's and addressee's name, organization, and facsimile and office telephone numbers. AID Form 330-7, FACSIMILE TRANSMITTAL COVER SHEET, may need additional modification for facsimile transmittals that contain SBU or classified information**.** (See Additional Help item, **Sample Facsimile Cover Sheet**)

b. Personnel Responsibility

The designated ISSO for unclassified information systems is responsible for implementing applicable security policies for the protection of non-secure facsimile equipment.

c. Internal Audit Trail Functions

(1) Machine-generated transmission journals must indicate, at a minimum, the date, time, number of pages forwarded, and facsimile number dialed.

(2) Machine-generated receipt journals must indicate, at a minimum, the transmitting device's phone number or some other location identifier, time, date, and number of pages sent.

(3) The designated ISSO must retain internal audit trail reports in a central file for a minimum of six months, and make them available for security reviews and audits. For details on USAID's records management program, see ADS 502. (See Mandatory Reference, **ADS 502**)

545.3.11.5 Facsimile Gateways Connected to Workstations or Servers

Effective Date: 12/22/1995

The following policies must be adhered to when facsimile gateways are connected to client workstations or servers:

a. IT Specialists/System Managers must ensure that the default setting for facsimile gateways is "access denied." Access to a facsimile gateway menu, functions, and messages is to be granted only on an individual user basis.

b. IT Specialists/System Managers must activate and maintain operating system-level audit trail capabilities to record facsimile gateway activity that occurs between their system and other entities. The IT Specialist/System Manager must also implement a facsimile transmission log that indicates, at minimum, the time, date, point of origination and destination, and number of pages transmitted.

(1) The designated ISSO must review the facsimile activity log at least monthly to assess accesses, billing accuracy, and security anomalies. The transmission log must be retained in a central file for at least six months.

(2) The designated ISSO must inform the ISSO for USAID of all security-related anomalies discovered during the review of facsimile gateway logs.

c. Facsimile gateway connections must be used only for the transmission of non-sensitive unclassified, nonrecord data. The transmission of classified material over facsimile gateway connections is a security violation and must be handled in accordance with 12 FAM 550. (See Mandatory Reference, **12 FAM 550**)

545.3.12 Networking and Connectivity Security

Effective Date: 04/25/2002

USAID's policy is to protect Agency networks and systems against unauthorized remote access. USAID permits only authorized, secure remote connections to Agency networked systems by implementing firewall and advanced remote user authentication

technology. System Managers must implement the controls described in this section, to the extent permitted by contemporary technology, on all interconnected systems within their area of responsibility.

a. Simultaneous connections between USAID networked multi-user systems and remote systems are not permitted, except when secured by an appropriate firewall, advanced remote user authentication system, or a combination of these security measures, as determined by M/IRM/TCO and approved by the ISSO for USAID.

(1) As USAID organizations implement electronic systems that will permit individuals or entities that deal with USAID the option to submit information or conduct transactions with the Agency electronically, IS security requirements must be included in all systems engineering efforts.

(2) Specific details of the Government Paperwork Elimination Act and guidance from the Office of Management and Budget (OMB) can be found in the Mandatory Reference, "The Government Paperwork Elimination Act" (GPEA), **Public Law 105-277**; as implemented by Office of Management and Budget (OMB) Procedures and Guidance published May 2, 2000.

b. Stand-alone (single-user) systems may be connected to remote systems. Appropriate controls, configured in accordance with specifications determined by M/IRM/TCO and approved by the ISSO for USAID, must be implemented to protect the availability, integrity, and if necessary confidentiality of the information stored on the stand-alone system.

c. Connections, including direct, dial-in, or Internet connections, between USAID networked multi-user systems and remote external systems are not permitted without an appropriate firewall, advanced remote user authentication system, or a combination of these security measures, as determined by M/IRM/TCO and approved by the ISSO for USAID.

d. Direct dial-in connections to the USAID General Support System (GSS) are not permitted except through the use of advanced user authentication technology as determined by M/IRM/TCO and approved by the ISSO for USAID.

e. Direct dial-in connections to individually controlled workstations or servers attached to the USAID GSS are not permitted. Dial-in connections to non-networked (stand-alone, single-user) systems are permitted when appropriate controls, configured in accordance with specifications determined by M/IRM/TCO and approved by the ISSO for USAID, are implemented to protect the availability, integrity, and if necessary the confidentiality of the information stored on the stand-alone system.

f. Dial-out only connections are permitted from workstations or systems connected to a USAID network when configured in accordance with specifications determined by M/IRM/TCO and approved by the ISSO for USAID.

g. M/IRM/TCO is responsible for designating, in writing, a Network Operations Manager, a network ISSO, and an alternate network ISSO to manage network security concerns for the USAID GSS.

h. The M/IRM/TCO Network Operations Manager and network ISSO are responsible for coordinating their security-related concerns and activities with the ISSO for USAID.

i. All users requesting access to the USAID GSS are required to meet the Agency's minimum personnel screening requirement for access to sensitive unclassified USAID information, as defined by the Office of Security, prior to being granted access to the USAID GSS.

545.4 MANDATORY REFERENCES

545.4.1 External Mandatory References

a. Relevant Federal Statutes

1. The Computer Fraud and Abuse Act of 1986, Public Law 99-474, as amended by the National Information Infrastructure Protection Act of 1996, Public Law 104-294

2. The Computer Security Act of 1987, Public Law 100-235, as amended by Public Law 104-106, National Defense Authorization Act (Fiscal Year 1996) Division E, Information Technology Management Reform (Clinger-Cohen Act), and see also 44 United States Code (U.S.C.) Chapter 35 {Coordination of Federal Information Policy} - amended October 30, 2000, by Government Information Security Reform [GISR] Subtitle G of the FY 2001 DoD Authorization Act, Public Law 106-398. GISR has been implemented by OMB M-01-08, Guidance On Implementing the Government Information Security Reform Act (January 16, 2001).

3. The Electronic Communications Privacy Act of 1986, Public Law 99-508, as amended

4. The Freedom of Information Act of 1966, Public Law 89-554, as amended

5. The Government Paperwork Elimination Act (GPEA), Public Law 105-277; as implemented by Office of Management and Budget (OMB) Procedures and Guidance published May 2, 2000

6. The Identity Theft and Assumption Deterrence Act of 1998, Public Law 105-318

7. (Section 587 of the Fiscal Year 1999) The Omnibus Appropriations Act, Public Law 105-277, as amended

8. The Omnibus Diplomatic Security and Anti-terrorism Act of 1986, as amended

9. The Privacy Act of 1974, Public Law 93-579, as amended

10. The Trade Secrets Act of 1948 & 1980, Public Law 96-349, as amended

b. Executive Orders (EOs)

1. EO 12968, "Access to Classified Information"

2. EO 12656, "Assignment of Emergency Preparedness Responsibilities"

3. EO 12958, "Classified National Security Information" (as amended)

4. EO 13103, "Computer Software Piracy" as amended

5. EO 13011, "Federal Information Technology"

6. EO 12829, "National Industrial Security Program" (as amended)

7. EO 10450, "Security requirements for Government employment"

c. Circulars, Handbooks, Instructions, Manuals, Regulations

1. DOD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria"

2. Foreign Affairs Handbook, 12 FAH-6 (OSPB Security Standards and Policy Handbook)

3. 12 Foreign Affairs Manual 090, Definitions of Diplomatic Security Terms

4. **12 Foreign Affairs Manual 500, Information Security**

5. **National Information Assurance Certification and Accreditation Process (NIACAP, National Security Telecommunications and Information Systems Security Instruction {NSTISSI} No. 1000)**

6. **The Office of Management and Budget (OMB) Circular A-130 Management of Federal Information Resources and its Appendix III, Security of Federal Automated Information Resources.**

7. **The Office of Management and Budget (OMB) Circular A-123, Management Accountability and Control (as revised.)**

8. **32 Code of Federal Regulations (CFR) Part 2004, "Safeguarding Classified National Security Information" and associated implementing guidance**

545.4.2 Internal Mandatory References

a. **AID Form 545-1, Unclassified Information Systems Access Request Acknowledgement**

b. **AID Form 545-2, Authorized Access List**

c. **AID Form 545-3, Unclassified Information System Compliance Review**

d. **AID Form 545-4, USAID Computer System Access & Termination Request**

e. **AID Form 545-5, USAID Sensitive Data Nondisclosure Agreement**

f. **AID Form 545-6, Visitors Log**

g. **ADS 502, The USAID Records Management Program**

h. **ADS 507, Freedom of Information Act (FOIA)**

i. **ADS 508, Privacy Act - 1974**

j. **ADS 509, Creating, Altering, or Terminating a System of Records (Records Pertaining to Individuals)**

k. **ADS 530, Emergency Planning Overseas**

l. **ADS 531, Continuity of Operations Program**

m. **ADS 541, Information Management**

n. **ADS 543, Corporate Information Systems**

o. **ADS 549, Telecommunications Management**

p. **ADS 550, End-User Applications**

q. **ADS 552, Classified Information Systems Security**

r. **ADS 561, Security Responsibilities**

s. **ADS 562, Physical Security Programs (Overseas)**

t. **ADS 565, Physical Security Programs (Domestic)**

u. **ADS 566, U.S. Direct-Hire and PASA/RSSA Personnel Security Program**

v. **ADS 567, Classified Contracts, Grants, Cooperative Agreements, and Contractor/Recipient Personnel**

w. **ADS 568, National Security Information and Counterintelligence Security Program**

x. **Contract Clause Guide for Unclassified Information System Security Systems and Services**

***y.** **Incident Response Guidance for Unclassified Information Systems**

z. **Information Systems Certification and Accreditation Process, Approval to Operate**

aa. **Information Technology Security Roles and Responsibilities**

***bb.** **Information System Security Rules of Behavior for All Computer Network (AIDNET) Users or "ISSO User Rules of Behavior" [this document is only available on the intranet. Please contact Rich Caporiccio, M/IRM/IPA, if you need a copy]**

cc. **M/IRM/IPA/ISS Security Plan Survey at http://inside.usaid.gov/M/IRM/ipa/iss/progmgmt/secplan/main.htm**

545.5 ADDITIONAL HELP

a. **Contingency Planning for Information Resources**

b. **Sample Facsimile Cover Sheet**

c. Suggested Warning Screen Messages

545.6 DEFINITIONS

Effective Date: 04/25/2002

The terms and definitions below have been included into the ADS Glossary. See the **ADS Glossary** for all ADS terms and definitions.

An asterisk next to a definition indicates that either the term is new or its definition has been revised.

Accreditation
The formal declaration by a Designated Security Approving Authority (DSAA) that an information system (IS) is approved to operate in a particular security mode using a prescribed set of safeguards to an acceptable level of risk. {Source: a USAID variation of the Federal term used in NSTISSI No. 1000} (Chapter 545)

audit
To conduct the independent review and examination of system records and activities. (Chapter 545)

authentication
(1) the verification of an individual's identity, a device, or other entity in a computer system as a prerequisite to allowing access to resources in a system;
(2) the verification of the integrity of data being stored, transmitted, or otherwise exposed to possible unauthorized modification. (Chapter 545)

availability
That state when information, programs and interfaces are obtainable within an acceptable period of time. (Chapter 545)

Certification
The comprehensive evaluation of the technical and nontechnical security features of an IS and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements. {Source: NSTISSI No. 1000} Note: IS is the acronym for information system; in addition, when the two terms “certification” and “accreditation” are used together, they are usually abbreviated as “C&A”; all these terms are listed in this glossary (Chapter 545)

Certification Authority (CA)
The USAID official who certifies that a particular information system (IS) has completed the Certification and Accreditation (C&A) process, and is ready for “Accreditation” by the Designated Security Accreditation Authority (DSAA). (Chapter 545)

Classified National Security Information (Classified Information)
Information that has been determined pursuant to EO 12958 or any predecessor order to require protection against unauthorized disclosure and is marked (confidential, secret, or top secret) to indicate its classified status when in documentary form. It is also referred to as classified information.

a. confidential: Information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

b. secret: Information of which the unauthorized disclosure could reasonably be expected to cause serious damage to the national security.

c. top secret: Information of which the unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security. (Chapters 545, 552, 562, 566, 567)

compartmented
The breaking down of sensitive data into small, isolated blocks to reduce the risk of unauthorized access. (Chapters 545, 552)

confidentiality
That state when information, programs and interfaces are held in confidence and protected from unauthorized disclosure. (Chapter 545)

connection
Any arrangement (intentional or otherwise) of hardware, software, firmware, peripherals, cabling, transceivers, etc. that supports or could enable system interoperability. (Chapter 545)

dedicated mode
The mode of operation in which the system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time. (Chapters 545, 552)

Designated Security Accreditation Authority (DSAA)
A USAID official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with “Designated Accreditation Authority - DAA” (used by most Federal agencies); DAA also may refer to a designated accrediting authority or a designated approving authority. {Source: This is a USAID-specific variation on a Federal Government term included in NSTISSI No. 9001} (Chapter 545)

encryption
Protecting information by encoding it through use of logarithmic coding keys. (Chapters 545, 552)

firewall
A system available in many configurations providing the necessary isolation between trusted and untrusted environments. (Chapter 545)

General Support System
An interconnected set of information resources under the same direct management control which share common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a LAN including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization. {Source: NSTISSI No. 1000; cites also OMB A-130} (Chapter 545)

identification
The process that enables recognition of an entity by a system, generally by the use of unique machine-readable user names. (Chapter 545)

Information System (IS)
The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. This term includes both automated and manual information systems; its acronym is "IS." (Source: a variation of a term from NSTISSI 4009) (Chapters 545, 552)

Information Technology Architecture
The term "information technology architecture" means an integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the agency's strategic goals and information resources management goals. (Source: 40 U.S.C. Section 1425) (Chapters 545, 552)

Information Technology (IT)
(A) The term ‘information technology', with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.

(B) The term ‘information technology' includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

(C) Notwithstanding subparagraphs (A) and (B), the term `information technology' does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. (Source: Clinger-Cohen Act) (Chapters 518, 541-548, 552)

integrity
That state when information, programs and interfaces remain free from accidental or malicious alteration or destruction. (Chapter 545)

Interim Approval To Operate (IATO)
Determination applied when a system does not meet the requirements stated in the SSAA [System Security Authorization Agreement], but mission criticality mandates the system become operational. The IATO is a temporary approval that may be issued for no more than a one-year period. {Source: NSTISSI No. 1000} (Chapter 545)

least privilege
The principle requiring that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error, or unauthorized use of an information system (IS). (Chapter 545)

magnetic media
Devices that employ magnetic materials and technology to record and store information in digital form, such as magnetic tapes, floppy disks, hard disks etc. (Chapters 545, 552)

major application
A major application means an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the system in which they operate. {Source: NSTISSI No. 1000; cites also OMB A-130} (Chapter 545)

Mission Critical System
The term "mission critical system" means any telecommunications or information system used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, that

a. Is defined as a national security system under section 5142 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1452);

b. Is protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive Order or an Act of Congress to be classified in the interest of national defense or foreign policy; or

c. Processes any information, the loss, misuse, disclosure, or unauthorized access to or modification of would have a debilitating impact on the mission of an agency. (Source: Public Law 106-398) (Chapters 545, 552)

National Security System
The term "national security system" means any telecommunications or information system operated by the United States Government, the function, operation, or use of which

a. Involves intelligence activities;

b. Involves cryptologic activities related to national security;

c. Involves command and control of military forces;

d. Involves equipment that is an integral part of a weapon or weapons system; or

e. Is critical to the direct fulfillment of military or intelligence missions. This final subcategory does not include does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (Source: 40 U.S.C.1452) (Chapters 545, 552)

network
Any collection of systems and the connections between them. (Chapter 545)

non-Agency system
A system that does not meet the entire definition for an Agency system, e.g. privately owned systems and systems operated by other USG agencies, foreign governments and private industry. (Chapter 545)

non-sensitive information
Any information that need not be safeguarded against disclosure, but must be safeguarded against tampering, destruction, or loss due to record value, utility, replacement cost or susceptibility to fraud, waste, or abuse (Source: DOD 5200.28 / NISTIR 4659). Examples of non-sensitive information are: Travel of the Administrator or Deputy Administrator and all other employees to or through a medium or low terrorist threat environment; and information, the disclosure of which, does not adversely affect the conduct of Federal programs or the privacy to which individuals are entitled (i.e., the information is so public it might appear in the newspaper). (Chapter 545)

optical media
Devices that employ optical technology to record and store information in digital form such as compact disks (CDs). (Chapter 545)

Program Manager
Government official responsible and accountable for the conduct of a Government program. A Government program may be large (e.g., may provide U.S. assistance to other nations); it may also be a support activity such as the Agency's personnel or payroll program. (Chapters 545, 552)

risk
A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting impact. {Source: NSTISSI No. 1000} (Chapter 545)

risk assessment
The process of analyzing threats to and vulnerabilities of an IS [information system] and the potential impact the loss of information or capabilities of a system would have on national security. The resulting analysis is used as a basis for identifying appropriate and cost-effective countermeasures. {Source: NSTISSI No. 1000} (Chapter 545)

risk management
The process concerned with the identification, measurement, control, and minimization of security risks in information systems to a level commensurate with the value of the assets protected. {Source: NSTISSI No. 1000} (Chapter 545)

Security Test and Evaluation (ST&E)
The examination and analysis of the safeguards required to protect an IS [information system], as they have been applied in an operational environment, to determine the security posture of that system. {Source: NSTISSI No. 1000} (Chapter 545)

Sensitive But Unclassified information (SBU)
A category of unclassified official information and material that is not national security information, and therefore is not classifiable, but nevertheless requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of the Agency to accomplish its mission, proprietary data, records requiring protection under the Privacy Act, and data not releasable under Sections 552 and 552a of Title 5 of the Freedom of Information Act.

SBU information includes, but is not limited to, information received through privileged sources and certain personnel, medical, personnel, commercial, and financial records, investigatory, visa, law enforcement, or other information which, if released, could result

in harm or unfair treatment to any individual or group, or could have a negative impact upon individual privacy, Federal programs, or foreign relations. (source: 12 FAM 540)

Examples of SBU include travel of agency employees to or through a high or critical terrorist threat environment; investigatory records compiled by an agency conducting lawful national security intelligence investigation (source: FOIA); and candid assessments of situations in a host country which could cause embarrassment if made public. Material of this type, which requires protection and limited dissemination, shall be designated by any official having signing authority for the material. (Chapters 545, 552, 562, 566, 567)

STU-III
Secure Telephone Units (Chapter 545)

system
An assembly of hardware and software configured for the purpose of processing, transmitting and receiving, storing and retrieving data; a system may include microcomputers, facsimiles, private branch exchanges, gateways and firewall equipment of any sort. (Chapter 545)

System Security Authorization Agreement (SSAA)
The SSAA is a formal agreement among the DSAA(s), certifier, IS user representative, and the program manager. It is used throughout the C&A process to guide actions, and to document decisions, security requirements, certification tailoring and level-of-effort, certification results, certifier's recommendation, and the approval to operate. {Source: NSTISSI No. 1000} Note: C&A is the acronym for Certification and Accreditation; DSAA is the acronym for Designated Security Accreditation Authority; and IS is the acronym for information system(s), all these terms are listed elsewhere in this glossary. (Chapter 545)

TEMPEST
The investigation, study, and control of compromising electromagnetic emanations from telecommunications and IS equipment. Sometimes refers to system components that use approved emanation suppression/containment systems for the processing and storage of classified national security information. (Chapters 545, 552, 562)

UNCLASSIFIED
Information that has not been determined pursuant to EO 12958 or any predecessor order to require protection against unauthorized disclosure and that is not designated as classified. (source: NTISSI 4009). A category of information that includes both Sensitive But Unclassified (SBU) and non-sensitive information and materials which at a minimum must be safeguarded against tampering, destruction, or loss. SBU information and materials must also be afforded additional protections commensurate with the sensitivity level of the data involved. (Chapters 545, 552)

USAID system
A system funded by the Agency and operated by or for the Agency and located in space owned or directly leased by the Agency or another agency of the USG. (Chapter 545)

validation
The process of applying specialized security test and evaluation procedures, tools, and equipment needed to establish acceptance for joint usage of an IS [information system] by one or more departments or agencies and their contractors. {Source: NSTISSI No. 1000} (Chapter 545)

verification
The process of comparing two levels of an IS [information system] specification for proper correspondence, e.g., security policy model with top-level specification, top-level specification with source code, or source code with object code. {Source: NSTISSI No. 1000} (Chapter 545)

vulnerability
A weakness (or weaknesses) in an IS [information system], system security procedures, internal controls, or implementation that could be exploited. {Source: NSTISSI No. 1000} (Chapter 545)

vulnerability assessment
A systematic examination of an IS [information system] or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. (Source: NSTISSI No. 1000) (Chapter 545)

545_050903_w052203